Chapter 1.8
Online Privacy, Vulnerabilities, and Threats:
A Manager's Perspective

Hy Sockel
DIKW Management Group, USA

Louis K. Falk
University of Texas at Brownsville, USA

ABSTRACT

There are many potential threats that come with conducting business in an online environment. Management must find a way to neutralize or at least reduce these threats if the organization is going to maintain viability. This chapter is designed to give managers an understanding, as well as the vocabulary needed to have a working knowledge of online privacy, vulnerabilities, and threats. The chapter also highlights techniques that are commonly used to impede attacks and protect the privacy of the organization, its customers, and employees. With the advancements in computing technology, any and all conceivable steps should be taken to protect an organization's data from outside and inside threats.

INTRODUCTION

The Internet provides organizations unparalleled opportunities to perform research and conduct business beyond their physical borders. It has proven to be a vital medium for worldwide commerce. Even small organizations now rely on Internet connectivity to communicate with their customers, suppliers, and partners. Today, employees routinely work from areas beyond their office's physical area. They regularly transport sensitive information on notebook computers, personal digital assistants (PDAs), smartphones, and a variety of storage media: thumb drives, CDs, DVDs, and even on floppies. It is not uncommon for employees to work offsite, at home, or out of a hotel room. Outside the office, they often use less

DOI: 10.4018/978-1-61350-323-2.ch1.8

than secure Internet connections—dial-up, cable, Internet cafés, libraries, and wireless.

Organizations often employ portals to share information with their stakeholders, however; these portals are not always secure from would be attackers. In order to protect the organization from vicious and malicious attacks, management needs to understand what they are up against. Even if the organization does not conduct any business on the Internet, they are still not out of harms way. Viruses, Trojans, and spyware can come from multiple sources; floppy discs, CDs, thumb drives, and even from mobile phones. To complicate the matter even more, the information technology (IT) environment at many organizations has become obscure—partially due to new regulations and industry standards. The standard has changed, it is no longer enough to be secure and protect the businesses assets, organizations need to be able demonstrate that they are compliant and that security is an ongoing concern; failure to do so could leave them facing stiff penalties (Forescout, 2007).

The purpose of this chapter is to address some of the potential threats that come with conducting business in an online environment. The chapter highlights the relationship between privacy and vulnerability and threats. It delves into techniques that are commonly used to thwart attacks and protect individuals' privacy. In the age of unrest and terrorism, privacy has grown even more important, as freedoms are compromised for security.

The news is loaded with stories about security breaches. For example:

In May of 2007, the news of the TJ Maxx security breach shook up the banking and retail industry. At first it was estimated that hackers had downloaded at least 45.7 million credit- and debit-card numbers; however, court filings indicated that number was closer to 96 million. Estimates for damage range from $216 million to $4.5 billion. The breach was blamed on extensive cyber thief activity within TJ Maxx's network from 2003 through June 2004 and then again from mid-May 2006 through mid-December 2006 (Schuman, 2007). However, others blame the breach on weak wireless security—Ou (2007) revealed that the "retailer's wireless network had less security than many people have on their home networks."

Another example is:

In April 5, 2002 hackers exploited vulnerabilities in a server holding a database of personnel information on California's 265,000 state employees. The state responded, and the world listened. California is one of the largest economies in the world, bigger than most countries. The attack included in its victims, the then Governor Grey Davis and 120 state legislators. The breach compromised names, social security numbers, and payroll information. In response, the state legislature enacted a security breach notification law Senate Bill (SB) 1386.

To put this in perspective, if online privacy is described in terms of a risk "triangle," the three corners are vulnerabilities, threats, and actions. Where actions represent anything the organization can (and should) do to mitigate attacks. Applications, like ships, are not designed and built to sit in a safe harbor, they were meant to be used in churning chaotic waters. It is important to understand threats and vulnerabilities enough to have a good idea to of what to expect, so that strategies and tools can be put in place to mitigate the consequences (Bumgarner & Borg, 2007).

VULNERABILITY

Software vulnerabilities are not going away, in fact they are increasing. According to the Coordination Center at Carnegie Mellon University (CERT, 2007) there was an average of over 10 vulnerabilities discovered every day in 2003 (3,784 in total). This number has jumped to over 5500 in the first nine months of 2007.